南京信息工程大学 实验（实习）报告

实验名称 DH协议 实验（实习）日期 2023/11/22 指导教师 高光勇

系 计算机 专业 奇安信 年级 2021 班次 1 姓名 朱宸扬 学号 202183760012

一、实验目的

通过实验熟练掌握DH协议，了解密钥协商协议的内涵，理解公钥密码算法程序设计的基本思路。

二、实验要求

1 编写DH协议算法

2 要求有对应的程序调试记录和验证记录

三、实验内容 (要求写出算法原理、实验核心代码及运行结果)

import random

import math

from random import choice

def getRandomPrime(Nmax):

isPrime = [0]\*(Nmax+1)

primeList = []

isPrime[2] = 1

for i in range(3,Nmax,2):

isPrime[i] = 1

for i in range(3,int(math.sqrt((Nmax+1)))+1,2):

if(isPrime[i] == 1):

for j in range(i\*i,Nmax+1,2\*i):

isPrime[j] = 0

for i in range(2,Nmax+1):

if (isPrime[i]==1):

primeList.append(i)

p , q = random.sample(primeList,2)

return p

#根据原根的性质求质数de原根

def getPrimaryRoot(p):

a = 2

while True:

mark = 0

if a \*\* (p - 1) % p == 1:

num = 2

while num < p - 1:

if a \*\* num % p == 1:

mark = 1

num += 1

if mark == 0:

return a

a += 1

def getA\_B(g,a,p):

return (g \*\* a) % p

def getKey(A\_B,a\_b,p):

return (A\_B\*\*a\_b) % p

if \_\_name\_\_ == "\_\_main\_\_":

p = getRandomPrime(200)

g = getPrimaryRoot(p)

rand\_a = random.randint(0, p - 1)

A = getA\_B(g, rand\_a, p)

rand\_b = random.randint(0, p - 1)

B = getA\_B(g, rand\_b, p)

alice\_key = getKey(B,rand\_a,p)

bob\_key = getKey(A,rand\_b,p)

print("step1: ","a:",rand\_a," ","g:",g," ","p:",p)

print("step2: ", "A:", A)

print("step3: ", "B:", B)

print("step4: ", "Alice\_key:", alice\_key)

print("step5: ", "Bob\_key:", bob\_key)

四、实验心得

通过这次实验，加深了对DH协议的理解，了解了primaryroot的意义